Introducción a la Criptografía Moderna

Introducción "Básica" de Teoría de Números, Álgebra Abstracta, Aritmética de Cuerpos Finitos,

"Lo necesario para el curso"

Rodrigo Abarzúa[†],

[†]Universidad de Santiago de Chile
rodrigo.abarzua@usach.cl

April 4, 2014

Divisibilidad

Definición

- *Si* **a** *y* **b** *son enteros, diremos que* **a** *divide a* **b** *(denotado por* $\mathbf{a} \mid \mathbf{b}$*) si existe un entero* **c** *tal que* $\mathbf{b}=\mathbf{ac}$.
- *Si no existe este* **c** *entonces* **a** *no divide a* **b** *(denotado por* $\mathbf{a} \nmid \mathbf{b}$*).*
- *Si* **a** *divide a* **b** *entonces diremos que* **a** *es un divisor de* **b** *y que* **b** *es divisible por* **a**.

Divisibilidad

Lema

Suponga que a, b, c, x, y *son enteros.*

1. *Si* $a|b$ *y* $x|y$ *entonces* $ax|by$.
2. *Si* $a|b$ *y* $b|c$ *entonces* $a|c$.
3. *Si* $a|b$ *y* $b \neq 0$, *entonces* $|a| \leq |b|$.
4. *Si* $a|b$ *y* $a|c$ *entonces* $a|bx + cy$.

Divisibilidad

Definición

Un entero positivo $\mathbf{p} > 1$ *es un número primo si y solo si los divisores de* $\mathbf{p}$ *son* 1 *y* $\mathbf{p}$. *Si* $\mathbf{p}$ *no es primo, entonces se dice un número compuesto.*

Divisibilidad

Teorema

Dados dos números enteros **a** *y* **b** *con* **b**$\neq 0$, *existe únicos enteros* **q** *y* **r** *tal que*

$$a = bq + r \quad y \quad 0 \leq r < |b|$$

Observación

Recordar que el número **q** *es el cuociente de* **a** *dividido por* **b**, *y* **r** *es el resto.*

Máximo Común Divisor, GCD

Definición

El máximo común divisor (GCD en inglés) de dos números **a** *y* **b** *no ambos cero, es el entero más grande que divide ambos* **a** *y* **b**. *Denotaremos por* $gcd(a, b)$ *como el máximo común divisor de* **a** *y* **b**.

Máximo Común Divisor, GCD

Definición

Dos enteros **a** *y* **b** *se dicen que son primos relativos o coprimos si el* $gcd(a, b) = 1$.

Lema

El máximo común divisor de dos enteros satisface las siguientes condiciones:

1. $gcd(a, b) = gcd(-a, b)$.
2. $gcd(a, b) = gcd(a - b, b)$.
3. *Si* $gcd(a, b) = d$, *entonces* $gcd(a/d, b/d) = 1$

Algoritmo Euclideano

Teorema

Dados dos números enteros **a** *y* **b**, *si* $a = bq + r$, *y* $0 \leq r < b$, *entonces* $gcd(a, b) = gcd(b, r)$.

Algoritmo Euclideano para el cálculo de $gcd(a, b)$

Algorithm 1: $gcd(a, b)$

`Input:` Dos enteros no negativos a y b con $a \geq b$.

`Output:` El $gcd(a, b)$.

1. **While** $b \neq 0$ **do**
2. $r \leftarrow a \bmod b$, $a \leftarrow b$, $b \leftarrow r$.
3. **End While**
4. **Return** a

Observación

El Algoritmo anterior tiene complejidad $O((\lg(n))^2)$ *operaciones de bit.*

Algoritmo Euclideano

Ejemplo

Utilice el algoritmo Euclideano para calcular el $gcd(4864, 3458)$

$$\begin{aligned}
4864 &= 1 \cdot 3458 + 1406 \\
3458 &= 2 \cdot 1406 + 646 \\
1406 &= 2 \cdot 646 + 114 \\
646 &= 5 \cdot 114 + 76 \\
114 &= 1 \cdot 76 + 38 \\
76 &= 2 \cdot 38 + 0.
\end{aligned}$$

Luego el $gcd(4864, 3458) = 38$

Algoritmo Euclideano Extendido

Teorema

Para dos enteros **a** *y* **b** *existen* **m** *y* **n** *tal que* $ma + nb = gcd(a, b)$.

Algoritmo Euclideano Extendido

Algorithm 2: $gcd(a, b)$ y enteros x e y tal que satisface $ax + by = d$.

`Input:` Dos enteros no negativos a y b con $a \geq b$.

`Output:` $d = gcd(a, b)$ y enteros x e y que satisfacen $ax + by = d$.

1. Si $b = 0$ entonces $d \leftarrow a$, $x \leftarrow 1$, $y \leftarrow 0$
2. **Return**(d, x, y).
3. $x_2 \leftarrow 1$, $x_1 \leftarrow 0$, $y_2 \leftarrow 0$, $y_1 \leftarrow 1$.
4. **While** $b > 0$ **do**
5. $\quad q \leftarrow \lfloor a/b \rfloor$, $r \leftarrow a - qb$, $x \leftarrow x_2 - qx_1$, $y \leftarrow y_2 - qy_1$.
6. $\quad a \leftarrow b$, $b \leftarrow r$, $x_2 \leftarrow x_1$, $x_1 \leftarrow x$, $y_2 \leftarrow y_1$, e $y_1 \leftarrow y$.
7. **End While**
8. $d \leftarrow a$, $x \leftarrow x_2$, $y \leftarrow y_2$.
9. **Return**(d, x, y).

Observación

El Algoritmo anterior tiene complejidad $O((\lg(n))^2)$ *operaciones de bit.*

Ejercicios

Utilizar el algoritmo Euclideano extendido para calcular el $gcd(4864, 3458)$ *y* x, y *tal que* $4864x + 3458y = gcd(4864, 3458)$

Solución: El $gcd(4864, 3458) = 38$ *y* $(4864)(32) + (3458)(-45) = 38$

Aritmética Modular

En esta sección presentaremos una pequeña introducción de la aritmética modular

Definición

Supongamos que **a**, **b** *y* **m** *son enteros, se dice que* **a** *es congruente a* **b modulo m** *denotado como*

$$a \equiv b (\bmod m)$$

si **m** *divide a* **a-b**. *El entero* **m** *es llamada el modulo de la congruencia.*

Aritmética Modular

Ejemplo

Observar los siguientes ejemplos:

- *Como* $9 = 23 - 14$*, por la definición implica que* $23 \equiv 14 (\bmod 9)$*. De hecho, cualquiera de dos números de la siguiente lista* $\{\dots, -4, 5, 14, 23, \dots\}$ *son congruentes modulo* 9*.*
- *Claramente si* $a \equiv b (\bmod m)$ *es lo mismo que* $a \equiv b (\bmod (-m))$*. Desde que solo se considera m un entero positivo.*

Aritmética Modular

Observación

La congruencia $a \equiv b \pmod{m}$ *significa que ambos* a *y* b *tienen el mismo resto al dividirlos por* m*. En efecto, podemos escribir*

$$a = q_1 m + r_1 \ \ y \ \ b = q_2 m + r_2$$

donde $r_1 = a \bmod m$ *y* $r_2 = b \bmod m$*.*
Por lo tanto

$$a - b = q_1 m + r_1 - (q_2 m + r_2) = (q_1 - q_2)m + (r_1 - r_2),$$

como r_1 *y* r_2 *son menores que* m*, entonces* $(r_1 - r_2)$ *también.*
Como $a \equiv b \pmod{m}$ *entonces* $a - b = km$ *para algún entero* k *entonces* $r_1 - r_2 = 0$*.*

Aritmética Modular

Observaciones

1. *Cuando se utilice la notación*

$$a \bmod m$$

   (sin parentesis) sera para denotar el resto cuando a *es dividido por* m, *es decir,* r_1 *en la observación de arriba. Si reemplazamos* a *por* $a \bmod m$, *diremos que* a *es reducido modulo* m.

2. *Algunos lenguajes de programación definen* $a \bmod m$ *como el resto en el rango* $-m+1, \ldots, m-1$ *teniendo el mismo signo de* a. *Por ejemplo,* $-18 \bmod 7$ *podría ser* -4, *pero también puede ser* 3. *En este curso siempre se definira* $a \bmod m$ *como no-negativo.*

Aritmética Modular

Teorema

Para todo $a, a_1, b, b_1, c \in \mathbb{Z}$. *Las siguientes propiedades se cumple:*

- $a \equiv b \pmod{n}$ *Si y solo si* a *y* b *tienen el mismo resto cuando se divide por* n.
- $a \equiv a \pmod{n}$ *(Reflexibidad).*
- *Si* $a \equiv b \pmod{n}$ *entonces* $b \equiv a \pmod{n}$ *(Simetria).*
- *Si* $a \equiv b \pmod{n}$ *y* $b \equiv c \pmod{n}$ *entonces* $a \equiv c \pmod{n}$ *(Transitividad).*
- *Si* $a \equiv a_1 \pmod{n}$ *y* $b \equiv b_1 \pmod{n}$, *entonces* $a + b \equiv a_1 + b_1 \pmod{n}$ *y* $ab \equiv a_1 b_1 \pmod{n}$.

Aritmética Modular

Ahora definiremos la aritmética modular o modulo $m : \mathbb{Z}_m$ se define como el conjunto $\{0, \ldots, m-1\}$, dotado de dos operaciones la adición $+$ y la multiplicaón $*$. Estas operaciones sobre $\mathbb{Z}_m$ operan exactamente como en los números reales, excepto que el resultado es reducido modulo m.

Ejemplo

Supongamos que calculamos $11 * 13$ *en* $\mathbb{Z}_{16}$. *Sabemos que* $11 * 13 = 143$, *al reducirlo modulo* 16 *es decir, escribimos* $143 = 8 * 16 + 15$, *entonces* $143 \bmod 16 = 15$, *luego* $11 * 13 = 15$ *en* $\mathbb{Z}_{16}$.

Existe una manera para representar un grupo finito. Utilizando las *tablas de Cayley*.

Ejemplo

La tabla de Cayley para el grupo $\mathbb{Z}_6$ *es:*

$+$	[0]	[1]	[2]	[3]	[4]	[5]
[0]	[0]	[1]	[2]	[3]	[4]	[5]
[1]	[1]	[2]	[3]	[4]	[5]	[0]
[2]	[2]	[3]	[4]	[5]	[0]	[1]
[3]	[3]	[4]	[5]	[0]	[1]	[2]
[4]	[4]	[5]	[0]	[1]	[2]	[3]
[5]	[5]	[0]	[1]	[2]	[3]	[4]

Aritmética Modular

Adición en $\mathbb{Z}_n$

Sea n un entero positivo. Dado que $\mathbb{Z}_n = \{0, 1, 2, \dots, n-1\}$. Si dados $a, b \in \mathbb{Z}_n$, entonces

$$(a+b) \bmod n = \begin{cases} (a+b) & \text{if } a+b < n, \\ \\ (a+b)-n & \text{if } a+b \geq n. \end{cases}$$

La definición de la adición y la multiplicación en $\mathbb{Z}_m$ satisface algunas propiedades que presentaremos sin demostración:

1. La adición es *cerrada*, es decir, para todo $a, b \in \mathbb{Z}_m$, $a+b \in \mathbb{Z}_m$.
2. La adición es *conmutativa*, es decir, para todo $a, b \in \mathbb{Z}_m$, $a+b = b+a$.
3. La adición es *asociativa*, es decir, para todo $a, b, c \in \mathbb{Z}_m$, $(a+b)+c = a+(b+c)$.
4. El *neutro aditivo* es el 0, es decir, para todo $a \in \mathbb{Z}_m$, $a+0 = 0+a = a$.
5. El *inverso aditivo* para algún $a \in \mathbb{Z}_m$ es $m-a$, es decir, $a+(m-a) = (m-a)+a = 0$ para todo $a \in \mathbb{Z}_m$.

Aritmética Modular

Multiplicación en $\mathbb{Z}_n$

Sea n un entero positivo. Si dados $a, b \in \mathbb{Z}_n$, entonces

$$(a * b) \bmod n = \begin{cases} (a * b) & \text{if } a + b < n, \\ (a * b) \bmod n & \text{if } a + b \geq n. \end{cases}$$

La definición de la adición y la multiplicación en $\mathbb{Z}_m$ satisface algunas propiedades que presentaremos sin demostración:

6. La multiplicación es *cerrada* es decir, si a y $b \in \mathbb{Z}_m$, entonces $ab \in \mathbb{Z}_m$
7. La multiplicación es *conmutativa*, es decir, para cada $a, b \in \mathbb{Z}_m$ entonces $ab = ba$.
8. La multiplicación es *asociativa*, es decir, para cada $a, b, c \in \mathbb{Z}_m$ entonces $(ab)c = a(bc)$
9. La *identidad multiplicativa* es el 1, es decir, para cada $a \in \mathbb{Z}_m$ $a * 1 = 1 * a = a$.
10. La multiplicación es *distributiva* sobre la adición, es decir,

$$a, b, c \in \mathbb{Z}_m, (a + b)c = (ac) + (ab) \text{ y } a(b + c) = (ab) + (ac)$$

Aritmética Modular

Observaciones

Las propiedades:

1, 3-5 *Se dice que* $\mathbb{Z}_m$ *forma una estructura algebraica llamada grupo, con la operación adición del grupo. Si se cumple la propiedad* **2** *se dice que el grupo es conmutativo.*

1-10 *Establecen que* $\mathbb{Z}_m$ *es un anillo, algunos ejemplos de anillos de cardinalidad infinita son* $\mathbb{Z}$, $\mathbb{R}$, $\mathbb{C}$. *En criptografía se esta interesado en anillos finitos.*

Aritmética Modular

Observación

Como en $\mathbb{Z}_m$ *existe el inverso aditivo, entonces podemos restar o sustraer elementos en* $\mathbb{Z}_m$. *Se define* $(a-b) \in \mathbb{Z}_m$ *como* $a+m-b \bmod m$. *De manera equivalente podemos calcular el* $a-b$ *y luego reducir modulo* m.

Ejemplo

Calcular $11-18 \in \mathbb{Z}_{31}$, $11+13 \bmod 31 = 24$.

Aritmética Modular

Definición

Sea $\mathbf{a} \in \mathbb{Z}_n$*. El inverso multiplicativo de* **a** *modulo* **n** *es un entero* $x \in \mathbb{Z}_n$ *tal que* $ax \equiv 1 \pmod{n}$*. Si este número existe, es único y diremos que* **a** *es invertible o una unidad, el inverso de* **a** *se denota por* $\mathbf{a}^{-1}$*.*

Definición

Dados $a, b \in \mathbb{Z}_n$*. La división de* **a** *por* **b** *modulo* **n** *es el producto de* **a** *y* $\mathbf{b}^{-1}$ *modulo* **n** *y si y solo si* **b** *es invertible modulo* **n**.

Aritmética Modular

Teorema

Sea $a \in \mathbb{Z}_n$. *Entonces* a *es invertible si y solo si* $gcd(a, n) = 1$.

Observación

Recordemos que el algoritmo Euclideano extendido nos permite calcular el $gcd(a, n)$ *y* p, q *tal que*

$$ap + nq = gcd(a, b).$$

Dado el teorema anterior si el $gcd(a, n) = 1$ *entonces el inverso*

$$a^{-1} (\bmod n) = p$$

Aritmética Modular

Definición

El grupo multiplicativo de $\mathbb{Z}_n$ *es* $\mathbb{Z}_n^* = \{a \in \mathbb{Z}_n | gcd(a, n) = 1\}$. *En particular si* **n** *es primo, entonces* $\mathbb{Z}_n^* = \{a | 1 \leq a \leq n - 1\}$.

Ejemplo

Consideremos el cuerpo finito $GF(5) = \{0, 1, 2, 3, 4\}$ *las siguientes tablas describen como sumar y multiplicar dos elementos*

+	0	1	2	3	4
0	0	1	2	3	4
1	1	2	3	4	0
2	2	3	4	5	1
3	3	4	5	0	2
4	4	5	0	1	3

Observar que los inversos aditivos son: $-0 = 0$, $-1 = 4$, $-2 = 3$, $-3 = 2$, $-4 = 1$

*	0	1	2	3	4
0	0	0	0	0	0
1	0	1	2	3	4
2	0	2	4	1	3
3	0	3	1	4	2
4	0	4	3	2	1

Observar que los inversos multiplicativos son: 0^{-1} *no existe,* $1^{-1} = 1$, $2^{-1} = 3$, $3^{-1} = 2$, $4^{-1} = 4$.

Un importante ejemplo de cuerpos primos es $GF(2)$, que es el cuerpos finito mas pequeño que existe.

Ejemplo

Consideremos el cuerpo finito $GF(2) = \{0, 1\}$. *La aritmetica del cuerpo es:*

Adición

$+$	0	1
0	0	1
1	1	0

Multiplicación

$*$	0	1
0	0	0
1	0	1

Calculo del inverso multiplicativo en $\mathbb{Z}_n$

Calculo del inverso multiplicativo en $\mathbb{Z}_n$

Algorithm 3: Dado $a \in \mathbb{Z}_n$ Calcula a^{-1} mod n si existe.

`Input:` $a \in \mathbb{Z}_n$.

`Output:` a^{-1} mod n si existe.

1. Use el algoritmo Euclideano extendido para encontrar los enteros x e y tal que $ax + ny = d$ donde $d = gcd(a, n)$.
2. **If** $d > 1$, **them**
3. a^{-1} mod n no existe.
3. **else**
4. **Return** x

Exponenciación Modular

El cálculo $a^k \bmod n$, es decir, la exponenciación modular es un algoritmo crucial para varios protocolos criptograficos, el siguiente algoritmo hace uso de la siguiente observación.

Dado k en su representacón binaria $k = \sum_{i=0}^{t} k_i 2^i$, donde cada $k_i \in \{0, 1\}$. Entonces

$$a^k = \prod_{i=0}^{t} a^{k_i 2^i} = (a^{2^0})^{k_0}(a^{2^1})^{k_1} \cdots (a^{2^t})^{k_t} \quad .$$

Exponenciación Modular

Algoritmo Cuadrados-y-Multiplicaciones para a^k mod n

Algorithm 4: Exponenciación Modular

`Input:` $a \in \mathbb{Z}_n$ y $k \in \mathbb{Z}_n$ con $0 \leq k < n$ y $k = \sum_{i=0}^{t} k_i 2^i$.

`Output:` El a^k mod n.

1. $b \leftarrow 1$.
2. **If** $k = 0$ **do**
3. **Return** b.
4. $A \leftarrow a$.
5. **For** i **from** 1 **to** t **do**
6. $A \leftarrow A^2$ mod n.
7. **If** $k_i = 1$ **then**
8. $b \leftarrow A \cdot b$ mod n.
4. **Return** b

Exponenciación Modular

Ejemplo

Utilizando el algoritmo anterior $5^{596} \bmod 1234 = 1013$

Complejidad de operaciones en $\mathbb{Z}_n$

Operación		Complejidad bit
Adición Modular	$(a + b) \bmod n$	$O(\lg n)$
Sustracción Modular	$(a - b) \bmod n$	$O(\lg n)$
Multiplicación Modular	$(a \cdot b) \bmod n$	$O((\lg n)^2)$
Inversión Modular	$a^{-1} \bmod n$	$O((\lg n)^2)$
Exponenciación Modular	$a^k \bmod n,\ k < n$	$O((\lg n)^3)$